FortiManager v5.0 Patch Release 4
Upgrade Guide

FortiManager v5.0 Patch Release 4 Upgrade Guide

September 13, 2013

02-504-214027-20130913

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Change Log

Date	Change Description
2013-09-13	Initial release.

FortiManager Firmware

This document provides an overview of FortiManager firmware and highlights general information you should be aware of prior to upgrading your FortiManager device. This guide is intended to supplement the *FortiManager Release Notes* documentation.

The following topics are included in this section:

Best practices

Before any firmware upgrade complete the following:

- Download the FortiManager firmware image and Release Notes document from the Customer Service & Support portal. Review the Release Notes including special notices, upgrade information, product integration and support, resolved and known issues.
- Prepare your FortiManager for upgrade, install any pending configurations, ensure your managed devices are running the appropriate firmware versions as documented in the firmware Release Notes.
- Backup your configuration file. It is recommended that you create a system backup file and save this configuration to your local computer. The device configuration file is saved with a .dat extension.

In VM environments, it is recommended that you take a *Snapshot* of the VM instance. In the event of an issue with the firmware upgrade, use the *Snapshot Manager* to revert to the *Snapshot*. To create a *Snapshot*, right-click the VM instance and select *Snapshot* > *Take Snapshot*.

- Plan a maintenance window to complete the firmware upgrade. If possible, you may want to set up a test environment to ensure that the upgrade does not negatively impact your network or managed devices.
- Once the upgrade is complete, test your FortiManager device to ensure that the upgrade was successful and that all managed devices are listed.

Firmware best practice: Stay current on patch releases for your current major release. Only upgrade to a new major release or version when you are looking for specific functionality in the new major release or version. For more information, see the *FortiManager Release Notes* or contact Technical Support.

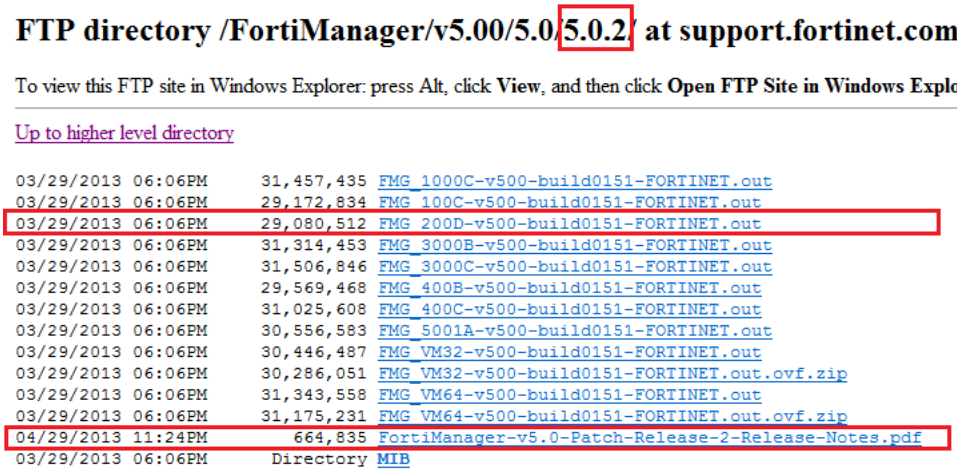
Firmware image naming convention

FortiManager firmware images on the Customer Service & Support portal FTP directory are organized by firmware version, major release, and patch release. The firmware images in the directories follow a specific naming convention and each firmware image is specific to the device model. For example, the FMG_200D-v500-build0151-FORTINET.out image found in the v5.0 Patch Release 2 directory is specific to the FortiManager 200D device model and the FMG_1000C-v400-build0700-FORTINET.out image found v4.0 MR3 Patch Release 7 directory is specific to the FortiManager 1000C device model.

Figure 1 shows the version 5.0 Patch Release 2 FTP directory and highlights the firmware image for the FortiManager 200D and the location of the *FortiManager v5.0 Patch Release 2 Release Notes*.

You can also download the Fortinet-FortiManager-FortiManager MIB file in this directory. The Fortinet Core MIB file is located in the main FortiManager v5.00 directory.

Figure 1: v5.0 Patch Release 2 FTP directory



FTP directory /FortiManager/v5.00/5.0/5.0.2/ at support.fortinet.com

To view this FTP site in Windows Explorer: press Alt, click **View**, and then click **Open FTP Site in Windows Explorer**.

Up to higher level directory

03/29/2013 06:06PM	31,457,435	FMG_1000C-v500-build0151-FORTINET.out
03/29/2013 06:06PM	29,172,834	FMG_100C-v500-build0151-FORTINET.out
03/29/2013 06:06PM	29,080,512	FMG_200D-v500-build0151-FORTINET.out
03/29/2013 06:06PM	31,314,453	FMG_3000B-v500-build0151-FORTINET.out
03/29/2013 06:06PM	31,506,846	FMG_3000C-v500-build0151-FORTINET.out
03/29/2013 06:06PM	29,569,468	FMG_400B-v500-build0151-FORTINET.out
03/29/2013 06:06PM	31,025,608	FMG_400C-v500-build0151-FORTINET.out
03/29/2013 06:06PM	30,556,583	FMG_5001A-v500-build0151-FORTINET.out
03/29/2013 06:06PM	30,446,487	FMG_VM32-v500-build0151-FORTINET.out
03/29/2013 06:06PM	30,286,051	FMG_VM32-v500-build0151-FORTINET.out.ovf.zip
03/29/2013 06:06PM	31,343,558	FMG_VM64-v500-build0151-FORTINET.out
03/29/2013 06:06PM	31,175,231	FMG_VM64-v500-build0151-FORTINET.out.ovf.zip
04/29/2013 11:24PM	664,835	FortiManager-v5.0-Patch-Release-2-Release-Notes.pdf
03/29/2013 06:06PM	Directory	MIB

FortiManager VM firmware

Fortinet provides FortiManager VM firmware images for both VMware ESX/ESXi and Microsoft Hyper-V Server 2008/2012 virtualization environments.

VMware ESX/ESXi

- FMG_VMxx-v500-buildxxxx-FORTINET.out: Download either the 32-bit or 64-bit firmware image to upgrade your existing FortiManager VM installations.
- FMG_VMxx-v500-buildxxxx-FORTINET.out.ovf.zip: Download either the 32-bit or 64-bit package for new FortiManager VM installations. The package contains a deployable Open Virtualization Format (OVF) virtual machine package for VMware ESX/ESXi installations and the fmg.vmdk and datadrive.vmdk virtual machine disk format files.

Microsoft Hyper-V Server

- FMG_VM64_HV-v500-buildxxxx-FORTINET.out: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- FMG_VM64_HV-v500-buildxxxx-FORTINET.out.hyperv.zip: Download the 64-bit package for a new FortiManager VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.

For more information see the FortiManager product datasheet available on the Fortinet web site, http://www.fortinet.com/products/fortimanager/virtualappliances.html.

Build numbers

FortiManager firmware images are generally documented as a three-digit build number. New FortiManager models may be released on a special branch based off of the regular FortiManager firmware release. As such, the build number found in the *System Settings* > *General* > *Dashboard, System Information* widget and the output from the `get system status` CLI command displays this four-digit special build number as the build number.

To confirm that you are running the proper build, the output from the `get system status` CLI command has a `Branch point:` field that displays the regular three-digit build number.

The following examples provide the output from the `get system status` CLI command for both a regular firmware release and a new model firmware release.

Example 1: Regular firmware release

```
Platform Type                    : FMG-VM
Version                          : v5.0-build0151 130328 (GA Patch 2)
Serial Number                    : FMG-VM0000000000
BIOS version                     : 04000002
Hostname                         : FMG-VM
Max Number of Admin Domains      : 10
Max Number of Device Groups      : 10
Admin Domain Configuration       : Disabled
FIPS Mode                        : Disabled
HA Mode                          : Stand Alone
Branch Point                     : 151
Release Version Information      :  (GA Patch 2)
Current Time                     : Wed Apr 24 12:14:08 PDT 2013
Daylight Time Saving             : Yes
Time Zone                        : (GMT-8:00)Pacific Time(US&Canada)
License Status                   : Valid
```

Example 2: New model firmware release

```
Platform Type                    : FMG-300D
Version                          : v5.0-build4020 130316
Serial Number                    : FMG-300D11000137
BIOS version                     : 04000002
Hostname                         : FMG-300D
Max Number of Admin Domains      : 300
Max Number of Device Groups      : 300
Admin Domain Configuration       : Enabled
FIPS Mode                        : Disabled
HA Mode                          : Stand Alone
Branch Point                     : 151
Release Version Information      : Patch Release 2
Current Time                     : Wed Apr 24 15:54:01 PDT 2013
Daylight Time Saving             : Yes
Time Zone                        : (GMT-8:00)Pacific Time(US&Canada)
License Status                   : Valid
```

Firmware upgrade and support information

The following table is for reference only. Review the applicable FortiManager releases notes prior to upgrading your FortiManager system.

The following table uses the naming convention '4.3.7', where the first digit reflects the version, the second digit reflects the major release, and the third digit reflects the patch release. For example, 4.3.7 is v4.0 MR3 Patch Release 7.

Table 1: FortiManager upgrade and support information

FortiManager Firmware Version	Build Number	Upgrade From	FortiOS Version Support
FortiManager 5.0			
5.0.5 Release Date: TBD			
FortiManager 5.0.5 is available for the following models:			
5.0.4 Release Date: 2013-09-13	0232	5.0.0 or later 4.3.0 or later	5.0.4 4.3.2 or later 4.2.0 or later
FortiManager 5.0.4 is available for the following models: FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-1000C, FMG-3000B, FMG-3000C, FMG-4000D, FMG-5001A, FMG-VM32, FMG-VM64, and FMG-VM64-HV.			
5.0.3 Release Date: 2013-07-10	0200	5.0.0 or later 4.3.0 or later	5.0.3 4.3.2 or later 4.2.0 or later
FortiManager 5.0.3 is available for the following models: FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-1000C, FMG-3000B, FMG-3000C, FMG-4000D, FMG-5001A, FMG-VM32, FMG-VM64, and FMG-VM64-HV. FMG-VM64-HV is released on the regular build.			
5.0.2 Release Date: 2013-03-28	0151	5.0.0 or 5.0.1 4.3.0 or later	5.0.2 4.3.2 or later 4.2.0 or later
FortiManager 5.0.2 is available for the following models: FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-1000C, FMG-3000B, FMG-3000C, FMG-5001A, FMG-VM32, and FMG-VM64. The FMG-300D is released on special build 4020. The FMG-4000D is released on special build 4019.			
5.0.1 Release Date: 2013-02-01	0121	5.0.0 4.3.0 or later	5.0.1 4.3.2 or later 4.2.0 or later
FortiManager 5.0.1 is available for the following models: FMG-100C, FMG-200D, FMG-400B, FMG-400C, FMG-1000C, FMG-3000B, FMG-3000C, FMG-5001A, FMG-VM32, and FMG-VM64. The FMG-300D is released on special build 4009.			
5.0.0 Release Date: 2012-11-01	0076	4.3.0 or later	5.0.0 4.3.2 or later 4.2.0 or later

Table 1: FortiManager upgrade and support information (continued)

FortiManager Firmware Version	Build Number	Upgrade From	FortiOS Version Support
FortiManager 5.0.0 is available for the following models: FMG-100C, FMG-200D, FMG-400B, FMG-400C, FMG-1000C, FMG-3000B, FMG-3000C, FMG-5001A, FMG-VM32, and FMG-VM64.			
FortiManager 4.3			
4.3.8 Release Date: TBD			
FortiManager 4.3.8 is available for the following models:			
4.3.7 Release Date: 2013-02-20	0700	4.3.1 or later 4.2.0 or later	4.3.5 or later 4.2.0 or later
FortiManager 4.3.7 is available for the following models: FMG-100, FMG-100C, FMG-200D, FMG-400A, FMG-400B, FMG-400C, FMG-1000C, FMG-3000, FMG-3000B, FMG-3000C, FMG-5001A, FMG-VM32, and FMG-VM64.			
4.3.6 Release Date: 2012-07-05	0673	4.3.1 or later 4.2.0 or later	4.3.2, 4.3.3, 4.3.4, 4.3.5, or 4.3.6 4.2.0 or later
FortiManager 4.3.6 is available for the following models: FMG-100, FMG-100C, FMG-200D, FMG-400A, FMG-400B, FMG-400C, FMG-1000C, FMG-3000, FMG-3000B, FMG-3000C, FMG-5001A, FMG-VM32, and FMG-VM64.			
4.3.5 Release Date: 2012-05-17	0658	4.3.1 or later 4.2.0 or later	4.3.2, 4.3.3, 4.3.4, or 4.3.5 4.2.0 or later
FortiManager 4.3.5 is available for the following models: FMG-100, FMG-100C, FMG-400A, FMG-400B, FMG-400C, FMG-1000C, FMG-3000, FMG-3000B, FMG-3000C, FMG-5001A, FMG-VM32, and FMG-VM64. Note: There is no image available for the FMG-200D.			
4.3.4 Release Date: 2012-04-06	0640	4.3.1 or later 4.2.0 or later	4.3.2, 4.3.3, or 4.3.4 4.2.0 or later
FortiManager 4.3.4 is available for the following models: FMG-100, FMG-100C, FMG-200D, FMG-400A, FMG-400B, FMG-400C, FMG-1000C, FMG-3000, FMG-3000B, FMG-3000C, FMG-5001A, FMG-VM32, and FMG-VM64.			
4.3.3 Release Date: 2012-03-15	0631	4.3.1 or later 4.2.0 or later	4.3.2 or 4.3.3 4.2.0 or later
FortiManager 4.3.3 is available for the following models: FMG-100, FMG-100C, FMG-400A, FMG-400B, FMG-400C, FMG-1000C, FMG-3000, FMG-3000B, FMG-3000C, FMG-5001A, FMG-VM32, and FMG-VM64.			
4.3.2 Release Date: 2011-12-13	0590	4.3.1 or later 4.2.0 or later	4.3.2 4.2.0 or later
FortiManager 4.3.2 is available for the following models: FMG-100, FMG-100C, FMG-400A, FMG-400B, FMG-1000C, FMG-3000, FMG-3000B, FMG-3000C, FMG-5001A, FMG-VM32, and FMG-VM64.			
4.3.1 Release Date: 2011-07-21	0524	4.3.0 4.2.0 or later	4.3.0 or 4.3.1 4.2.0 or later
FortiManager 4.3.1 is available for the following models: FMG-100, FMG-100C, FMG-400A, FMG-400B, FMG-1000C, FMG-3000, FMG-3000B, FMG-3000C, FMG-5001A, and FMG-VM32. FMG-VM32 is released on special build 6172.			
4.3.0 Release Date: 2011-06-30	0514	4.2.1 or later	4.3.0 4.2.0 or later

Table 1: FortiManager upgrade and support information (continued)

FortiManager Firmware Version	Build Number	Upgrade From	FortiOS Version Support
FortiManager 4.3.0 is available for the following models: FMG-100, FMG-100C, FMG-400A, FMG-400B, FMG-1000C, FMG-3000, FMG-3000B, FMG-3000C, and FMG-5001A.			
FortiManager 4.2 is no longer supported (EOS) as of April 03, 2013.			

In version 5.0, FortiClient endpoint agent configuration and management are now handled by the FortiGate Endpoint Control feature. You can configure your FortiGate device to discover new devices on your network, enforce FortiClient registration, and deploy a pre-configured endpoint profile to connected devices. This feature requires a FortiGate device running FortiOS v5.0.0 or later.

For more information, see the *Device and Client Reputation for FortiOS 5.0 Handbook* available at http://docs.fortinet.com.

FortiManager v5.0.0 introduced a new hard disk drive partition layout which is required for optimal usage and performance. Following an upgrade to FortiManager v5.0.0 or later, a backup must be made and then the disk must be reformatted with following command:

```
execute format {disk | disk-ext4}
```

A format will erase all local logs, and FortiGuard database information. Backup any local event logs that you wish to keep. The FortiManager will then need to re-download all of the AV/IPS/AS/WF objects from the FortiGuard Distribution Servers (FDS) which may take up to half a day. During that time managed devices will not be able to obtain these services from the FortiManager. You should configure devices to point to a backup FortiManager or the FDS for these services

When upgrading from FortiManager v4.0 MR2 EMS mode, you must run the *Import Wizard* for each managed device to ensure all rules and policies are added to the FortiManager.

Upgrade Information

This section outlines the general firmware upgrade steps. The following topics are included in this section:

- General firmware upgrade steps
- Upgrading the FortiManager firmware for an operating cluster
- Downgrading to previous firmware versions

Please review the *Firmware Release Notes* prior to upgrading. For more information on upgrading your FortiManager device, see the *FortiManager Administration Guide* at http://docs.fortinet.com.

General firmware upgrade steps

The following table lists the general firmware upgrade steps.

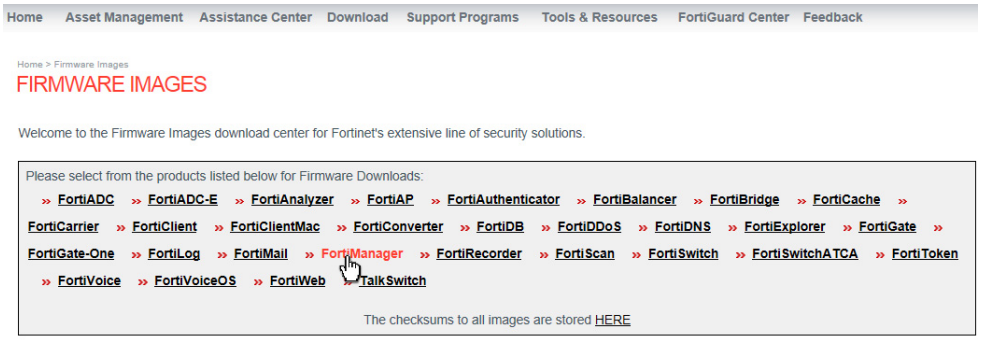
Table 2: Upgrade steps

Step 1	Prepare your FortiManager for upgrade.
Step 2	Backup your FortiManager system configuration. For FortiManager VM, take a *Snapshot* of the VM instance.
Step 3	Transfer the FortiManager firmware image to your FortiManager device.
Step 4	Log into your FortiManager Web-based Manager to verify the upgrade was successful.

Step 1: Prepare your FortiManager for upgrade

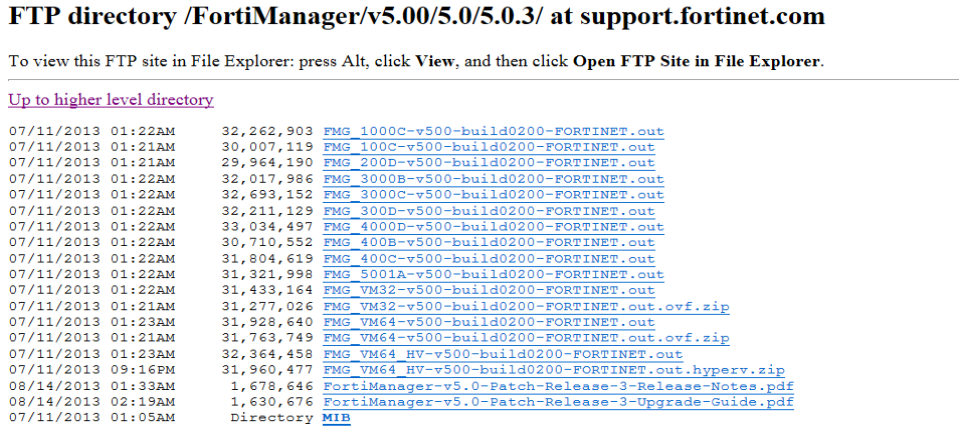
1. Install any pending configurations.
2. Make sure all managed devices are running the supported firmware versions as stated in the *Firmware Release Notes*.
3. Log in to the Customer Service & Support portal at https://support.fortinet.com.
4. In the *Download* section of the page, select *Firmware Images*, and select *FortiManager.*

Figure 2: Firmware images page



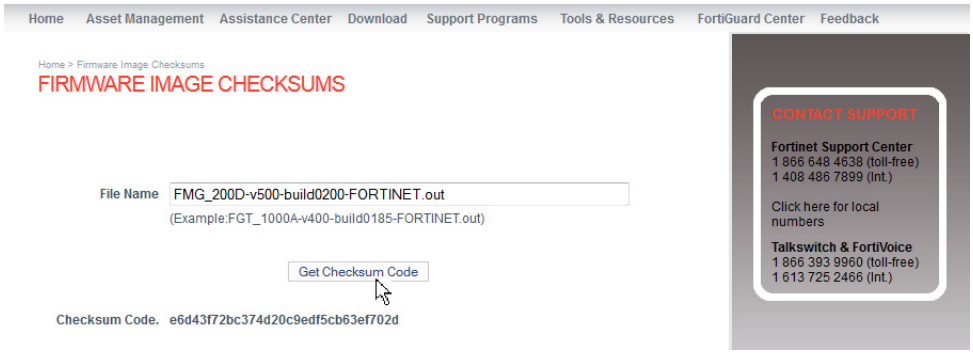
5. Browse to the appropriate FTP directory to download the firmware image and Release Notes document.

Figure 3: Example FTP directory



6. To verify the integrity of the download, go back to the *Download* section of the login page, then select the *Firmware Image Checksums* link.

Figure 4: Firmware image checksums page

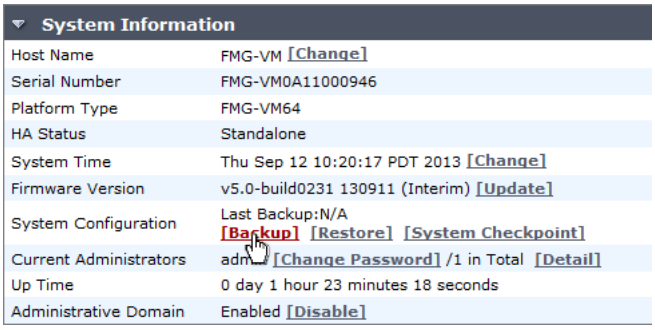


7. Enter the file name and select *Get Checksum Code* to get the firmware image checksum code. Compare this checksum with the checksum of the firmware image.

Step 2: Backup your FortiManager system configuration

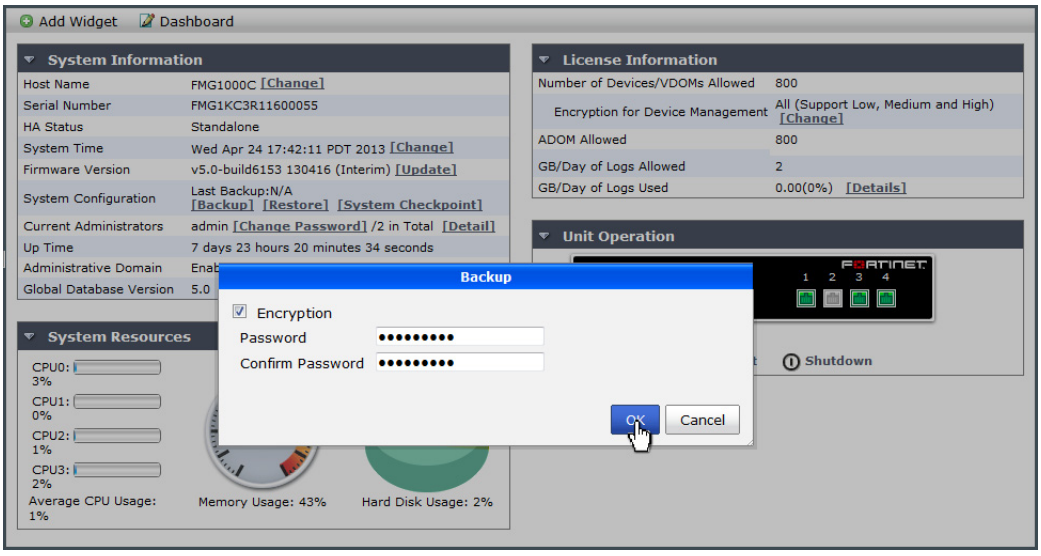
1. Go to *System Settings* > *Dashboard*.
2. Select *Backup* in the *System Information* widget.

Figure 5: System information widget



The *Backup* dialog box opens.

Figure 6: Backup dialog box



3. Select the checkbox to encrypt the backup file and enter a password.

When selecting to encrypt the backup configuration file, the same password used to encrypt the file will be required to restore this backup file to the FortiManager device.

4. Select *OK* and save the backup file on your local computer.

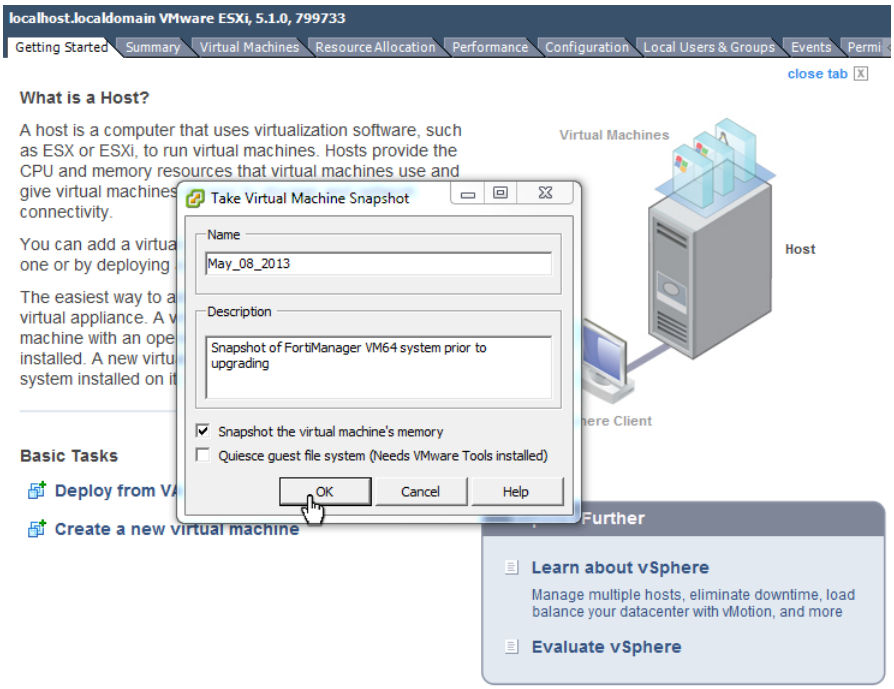
Optionally, you can backup the configuration file to a FTP, SFTP, or SCP server using the following CLI command:

```
execute backup all-settings {ftp | sftp} <ip> <path/filename save to
    the server> <username on server> < password> <crptpasswd>
execute backup all-settings scp <ip> <path/filename save to the
    server> <SSH certificate> <crptpasswd>
```

For more information, see the *FortiManager v5.0 Patch Release 4 CLI Reference*.

5. In VM environments, it is recommended that you take a *Snapshot* of the VM instance. In the event of an issue with the firmware upgrade, use the *Snapshot Manager* to revert to the *Snapshot*. To create a *Snapshot*, right-click the VM instance and select *Snapshot* > *Take Snapshot*.

Figure 7: Snapshot of FortiManager VM



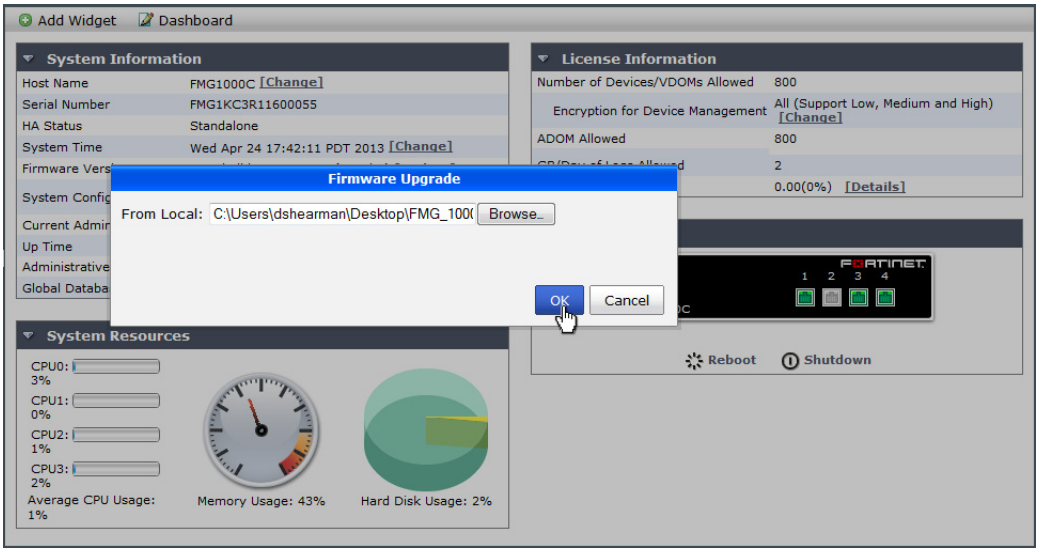
For information on taking snapshots in Microsoft Hyper-V Server environments, see the Microsoft Server online help.

Step 3: Transfer the firmware image to your FortiManager device

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, in the *Firmware Version* field, select *Update*.

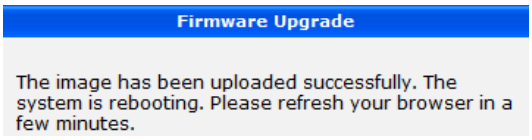
The *Firmware Upgrade* dialog box opens.

Figure 8: Firmware upgrade dialog box



3. Select *Browse* to locate the firmware package (`.out` file) that you downloaded from the Customer Service & Support portal and select *Open*.
4. Select *OK*. Your FortiManager will upload the firmware image and you will receive the following message.

Figure 9: Firmware upgrade successful dialog box



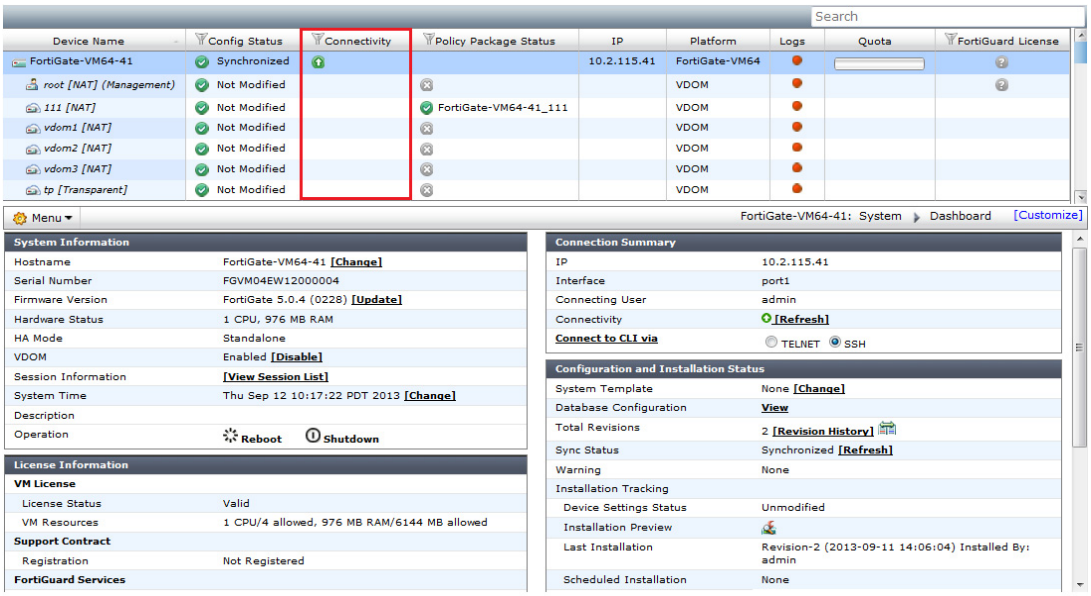
Optionally, you can upgrade firmware stored on an FTP or TFTP server using the following CLI command:

```
execute restore image {ftp | tftp} <file path to server> <IP of
    server> <username on server> <password>
```

Step 4: Verify the upgrade

1. Refresh the browser and log back into the device.
2. Launch the *Device Manager* module and make sure that all formerly added devices are still listed.
3. Select each ADOM and make sure that managed devices reflect the appropriate connectivity state. Optionally, go to *System Settings* > *All ADOMs*.

Figure 10: Device connectivity



4. Launch other functional modules and make sure they work properly.

Upgrading the FortiManager firmware for an operating cluster

You can upgrade the FortiManager firmware of an operating FortiManager cluster in the same was a upgrading the firmware of a standalone FortiManager unit. During the firmware upgrade procedure, you connect to the primary unit Web-based Manager or CLI to upgrade the firmware.

Similar to upgrading the firmware of a standalone FortiManager unit, normal FortiManager operations are temporarily interrupted while the cluster firmware upgrades. As a result of this interruption, you should upgrade the firmware during a maintenance window.

To upgrade FortiManager HA cluster:

1. Log into the primary unit Web-based Manager using the `admin` administrator account.
2. Upgrade the primary unit firmware. The upgrade is synchronized between the primary device and backup devices.

Administrators may not be able to connect to the FortiManager Web-based Manager until the upgrade synchronization process is complete. During the upgrade, using SSH or telnet to connect to the CLI may also be slow, however use the console to connect to the CLI.

Downgrading to previous firmware versions

FortiManager does not provide a full downgrade path. You can downgrade to a previous FortiManager firmware release via the Web-based Manager or CLI. A system reset is required after the firmware downgrading process has completed.

All configuration will be lost after downgrading the device. For FortiManager devices with hard drives installed, the hard drives will be formatted.

To re-initialize a FortiManager use the following CLI commands via a console port connection:

```
execute reset all-settings
execute format {disk | disk-ext4}
```